CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1, 2, 6-9, 11, 22-24, 28, 31, 32, 43, 46-47, and 49.
- After this Amendment: 1-2, 7-9, 11, 22-24, 28, 31-32, 43, 46-47, 49, and 50.

Non-Elected, Canceled, or Withdrawn claims: Claim 6

Amended claims: Claims 1, 2, 7-9, 11, 22-24, 28, 31, 32, 46-47, and 49.

New claims: Claim 50

This listing of claims replaces all prior versions, and listings, of claims in the Application.

Listing of Claims:

1. (Currently Amended) A method comprising:

generating, at a content publisher configured to provide digital rights management, a formal license for content that includes:

a decryption key for decrypting the content; and

access rules for accessing the content; and

configuring a plurality of license authorities to provide a plurality of partial licenses, wherein:

each said license authority provides a respective said partial license; and

the plurality of partial licenses are combinable to form the formal license;

wherein the configuring includes:

generating, at the content publisher, a pre-license from the formal license by encrypting the formal license utilizing an asymmetric encryption algorithm having a public key and a private key, wherein the formal license, the pre-license and the public key are denoted, respectively, as "license", "prel" and "PK" as follows:

$$prel = (license)pk;$$

dividing the private key SK into m partial secret shares according to a (k, m) threshold secret sharing scheme by[[:]]

generating a sharing polynomial f(x) being represented as follows:

f(x) = ao + a1x + …+ ak-1 xk-1 , where ao = SK~~; and~~

~~calculating each said partial secret share, denoted as Si, for a respective said license authority, denoted by idi, in which i = 1, …, m, as follows:~~

$$S_i = f(id) \bmod (\phi N),$$

~~where N is a RSA modulus and $\phi(N)$ is a Euler totient function;~~ and

transmitting the pre-license and a respective said partial secret share from the content publisher to a respective said license authority, wherein each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license, and wherein each said license authority is configured to verify the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme in which *k* public witnesses of the sharing polynomial's *f(x)* coefficients (denoted as $\{g^{a_0},\cdots;g^{a_{k-1}}\}$, where $g \in Z_N$) are communicated to each said license authority id_i to verify validity of a respective said partial secret share S_i by determining if the following equation holds:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \text{ mod N.}$$

2. (Currently Amended) A method as described in claim [[0]] 1, wherein the plurality of partial licenses is provided according to a (*k*, *m*) threshold secret sharing scheme in which:

a number *k* said partial licenses are combinable to form the formal license; and

knowledge of any $k-1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

3-6. (Canceled)

7. (Currently Amended) A method as described in claim [[0]] 1, further comprising packaging the content to include one or more network addresses that are suitable for locating each said license authority.

8. (Currently Amended) A method as described in claim [[0]] 1, wherein each said license authority is communicatively coupled to a peer-to-peer network.

9. (Currently Amended) A method as described in claim [[0]] 1, wherein the plurality of license authorities are configured based on a consideration such that at least one said license authority provides two or more said partial licenses, wherein the consideration is selected from the group consisting of:

security of the at least one said license authority against unauthorized access;

load sharing of the plurality of license authorities;

availability of each said license authority;

network availability of each said license authority;

hardware resources of each said license authority;

software resources of each said license authority; and

any combination thereof.

10. (Canceled)

11. (Currently Amended) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim [[0]] 1.

12-21. (Canceled)

22. (Currently Amended) A method comprising:

obtaining a plurality of partial licenses over a network at a client device executing a content player from a plurality of license authorities, wherein each said partial license is provided, respectively, by a different said license authority; and

forming a formal license from the plurality of partial licenses at the client device, wherein the formal license includes access rules and a decryption key for accessing content,

wherein:

the plurality of partial licenses are obtained from the plurality of license authorities at the client device by:

calculating the partial license preli by each said license authority idi from a partial secret share Si and a pre-license prel according to the following equation:

$$prel_i = (prel)^{S_i} \text{ mod N;}$$

generating a random number u to calculate A1 = gu, A2 = prelu, r = u – c * Si, and

$$c = hash\,(g^{S_i}, prel_i, A_1, A_2)\text{; and}$$

communicating the partial license preli, A1, A2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses at the client device by:

determining if k correct partial licenses have been received by validating each said partial license preli by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \text{ mod N}$$

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \cdots; g^{a_{k-1}}\}$, that was utilized to generate the partial secret share Si, where $g \in Z_N$,

applying $c = hash(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license preli, and if so, each said partial license preli is valid; and

combining the plurality of partial licenses to form the formal license at the client device, denoted as license, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$
$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}.$

23. (Currently Amended) A method as described in claim [[0]] 22, wherein the obtaining includes:

examining the content to find a plurality of network addresses of a plurality of license authorities;

requesting the plurality of partial licenses from the plurality of license authorities; and

receiving one or more communications having one or more said partial licenses that are provided by each said license authority.

24. (Currently Amended) A method as described in claim [[0]] 22, wherein the forming includes combining the plurality of partial licenses to form the formal license.

25-27. (Canceled)

28. (Currently Amended) One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim [[0]] 22.

29-30. (Canceled)

31. (Currently Amended) A method comprising:

configuring, at a content publisher configured to provide digital rights management, a plurality of license authorities in a first arrangement to provide a plurality of partial licenses, wherein:

each said license authority provides at least one said partial license; and

the plurality of partial licenses are combinable to form a formal license that includes access rules and a decryption key for content; and

updating, at the content publisher, the first arrangement to form a second arrangement such that:

each said license authority in the second arrangement provides at least one of a plurality of updated partial licenses that are combinable to form the formal license; and

the partial licenses provided in the first arrangement are not combinable with the updated partial licenses to form the formal license;

wherein the updating is performed by:

generating a random (k, m) sharing by each license authority i using a random update polynomial fi, update(x), wherein:

$$f_{i,update}(x) = b_{i,1}x + \ldots + b_{i,k-1}x^{k-1} \text{ mod } \phi(N);$$

and

distributing a subshare Si,j by each said license authority i such that each said license authority i has a respective said subshare Si,j from another said license authority wherein:

the subshare $S_{i,j} = f_{i,update}(j)$, $j = 1,\cdots,m$ is calculated by each said license authority i;

the subshare Si,j is added to the original share S_i of each said license authority to form a new updated share

$$S_i' = S_i + \sum_{j=1}^{m} S_{j,i}$$; and

a new secret sharing polynomial fnew(x) is formed which is a summation of an original polynomial f(x) utilized to generate the plurality of partial licenses in the first arrangement and each of the randomly generated polynomials fi,update(x).

32. (Currently Amended) A method as described in claim [[0]] 31, wherein the updating is performed periodically.

33-42. (Canceled)

43. (Previously Presented) A client device comprising:

a processor; and

memory configured to maintain:

packaged content that includes one or more network addresses that are suitable for locating a plurality of license authorities, wherein each said license authority stores one or more partial licenses;

a content player that is executable on the processor to output content; and

a digital rights management module that is executable on the processor to:

obtain the partial licenses from the plurality of license authorities utilizing the one or more network addresses; and

form a formal license from the obtained partial licenses, wherein the formal license provides access to the packaged content for output by the content player;

obtain the partial licenses from the plurality of license authorities, wherein each said license authority provide a respective said partial license by:

calculating the partial license preli by each said license authority idi from a partial secret share Si and a pre-license prel according to the following equation:

$$prel_i = (prel)^{S_i} \text{ mod N;}$$

generating a random number u to calculate A1 = gu, A2 = prelu, r = u – c * Si, and

$c = hash\,(g^{S_i}, prel_i, A_1, A_2)$; and

communicating the partial license preli, A1, A2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by validating each said partial license preli by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}} \text{ mod N}$$

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \cdots; g^{a_{k-1}}\}$, that was utilized to generate the partial secret share Si, where $g \in Z_N$,

applying $c = hash(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license preli, and if so, each said partial license preli is valid; and

combining the plurality of partial licenses to form the formal license, denoted as license, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$
$$= (prel)^{SK} = ((license)^{PK})^{SK} \bmod N,$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}.$

44-45. (Canceled)

46. (Currently Amended) A client device as described in claim [[0]] 43, wherein the one or more network addresses include a proxy address for locating a network address of each said license authority.

47. (Currently Amended) A client device as described in claim [[0]]

43, wherein the one or more network addresses include a network address of each said license authority.

48. (Canceled)

49. (Currently Amended) A method comprising:

receiving, ~~a formal license~~ at a license authority executing a license module, a formal license from a content publisher, the formal license including a decryption key and access rules relating to particular content, wherein the access rules specify a plurality of time durations to access particular content based on respective payment amounts;

receiving a request at the license authority from a client device for a number of partial licenses related to the particular content;

sending a request from the license authority to the client device for additional information specifying an output duration to access the particular content;

generating the number of partial ~~licens~~e licenses at the license authority based on the formal license and a response received from the client device specifying the output duration, wherein the number of partial licenses generated at the license authority is based on security safeguards of the license authority relative to security safeguards of a plurality of additional license authorities; and

sending the number of partial ~~license~~ licenses to the client device.

50. (New) A method comprising:

receiving content at a client device from a content publisher, wherein the client device is configured to execute a digital rights management module;

receiving a request to output the content at the client device;

determining, at the client device, if a valid formal license is available for the content at the client device, wherein the valid formal license is read to output the content;

obtaining, at the client device, a plurality of partial licenses from a plurality of license authorities when the valid formal license is not available at the client device, wherein the client device receives one partial license from a first number of the plurality of license authorities and the client device receives more than one license from a second number of the plurality of license authorities; and

combining the plurality of partial licenses at the client device to form the valid formal license.